

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-098774

(43)Date of publication of application : 14.04.1998

(51)Int.Cl. H04Q 7/38  
H04Q 7/34

(21)Application number : 09-205859

(71)Applicant : SIEMENS AG

(22)Date of filing : 31.07.1997

(72)Inventor : LINDER HERMANN DIPL ING

(30)Priority

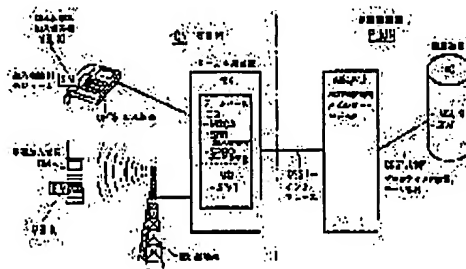
Priority number : 96 19630920 Priority date : 31.07.1996 Priority country : DE

## (54) METHOD AND DEVICE FOR AUTHENTICATING SUBSCRIBER AND/OR CODING INFORMATION

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a method and a device for subscriber authentication which enable a protecting means to be used at cost as low as possible even in another communication network connected to a mobile radio network respectively.

**SOLUTION:** The method and device are for authenticating a subscriber and/or coding information, a mobile radio network (PLMN) for a subscriber of another communication network(CN) prepares protection parameters (SPAR) through an interface (DSS1+) connecting both communication networks, and a subscriber of the mobile radio network needs not registers itself in at least one subscriber data base(DB) of the mobile radio network. At this time, the subscriber of the other communication network is identified by a subscriber identification module(SIM) of a subscriber station (UPTD, DM) and recorded in the subscriber data base of the other communication network. Protection parameters for a subscriber recorded in a leased network are requested through an interface, prepared by an authentication device (AC) of the mobile radio network, and transmitted to the leased network through the interface.



## LEGAL STATUS

[Date of request for examination] 31.07.1997

[Date of sending the examiner's decision of rejection] 16.05.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

**BEST AVAILABLE COPY**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-98774

(43) 公開日 平成10年(1998) 4月14日

(51) Int.Cl. <sup>8</sup>	識別記号	F I		
H 0 4 Q	7/38	H 0 4 B	7/26	1 0 9 S
	7/34	H 0 4 Q	7/04	C

審査請求 有 請求項の数 8 O L (全 7 頁)

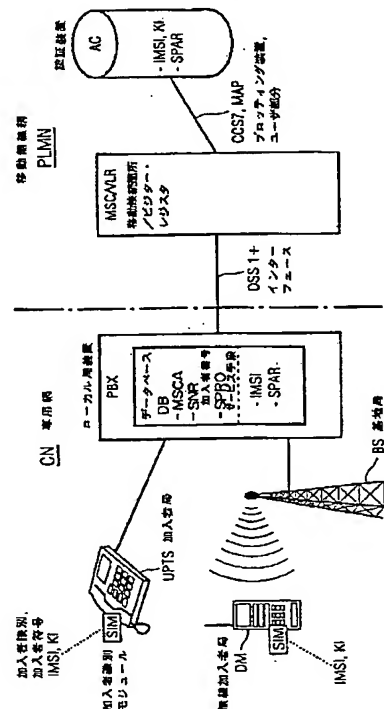
(21) 出願番号	特願平9-205859	(71) 出願人	396026260 ジーメンス アクティエンゲゼルシャフト ドイツ ミュンヘン D-80333 ヴィッ テルスバッハーブラッツ 2
(22) 出願日	平成9年(1997) 7月31日	(72) 発明者	ヘルマン リンダー オーストリア ドルフエン 84405 ジョ セフマーティン パウアー ストラッセ
(31) 優先権主張番号	1 9 6 3 0 9 2 0 . 4	(74) 代理人	弁理士 萩原 誠
(32) 優先日	1996年 7月31日		
(33) 優先権主張国	ドイツ (D E)		

(54) 【発明の名称】 加入者を認証するための及び／又は情報をコード化するための方法及び装置

(57) 【要約】

【課題】 保護手段が、それぞれ移動無線網に接続された別の通信網においても可能な限りわずかなコストで使用する事の出来る加入者認証方法及び装置を提供する。

【解決手段】 加入者を認証するための及び／又は情報をコード化するための方法及び装置であって、保護パラメータ (S P A R) が別の通信網 (C N) の加入者のための移動無線網 (P L M N) によって両通信網を接続しているインターフェース (D S S 1+) を介し準備されており、しかも移動無線網の加入者は、移動無線網の少なくとも1つの加入者データベース (D B) に加入者記録をする必要がない。その際別の通信網の加入者は、加入者局 (U P T S, D M) の加入者識別モジュール (S I M) によって識別され、かつ別の通信網の加入者データベースに記録される。専用網に記録された加入者のための保護パラメータは、インターフェースを介して要求され、移動無線網の認証装置 (A C) によって準備されかつインターフェースを介して専用網に伝送される。



## 【特許請求の範囲】

【請求項 1】 加入者を認証するための及び／又は情報をコード化するための方法であって、

移動加入者が、移動無線網 (PLMN) に対し加入者局に含まれる加入者識別モジュール (SIM) によって識別されかつ移動無線網 (PLMN) の少なくとも 1 つの加入者データベースで処理されて認証装置 (AC) に登録されており、該認証装置 (AC) から加入者データを保護するため、移動加入者に対しそれぞれ保護パラメータ及び保護アルゴリズムが準備されている形式のものにおいて、

—インターフェース (DSS1+) を介し移動無線網 (PLMN) に接続された別の通信網の加入者を、加入者識別モジュール (SIM) によって識別しかつ少なくとも別の通信網 (CN) の加入者データベース (DB) で処理し、

—別の通信網 (CN) の処理された加入者のための保護パラメータ (SPAR) をインターフェース (DSS1+) を介して要求し、移動無線網 (PLMN) の認証装置を、加入者の記録を移動無線網 (PLMN) の加入者データベース (HLR) で行うことなしに、インターフェース (DSS1+) によって準備しかつインターフェース (DSS1+) を介し別の通信網に伝送し、  
—別の通信網 (CN) の加入者のための認証及び／又は情報のコード化を、移動無線網 (PLMN) によって受信された保護パラメータに基づいて前記別の通信網 (CN) で実行することを特徴とする方法。

【請求項 2】 それぞれの保護パラメータ (SPAR) を準備する移動無線網 (PLMN) の認証装置 (AC) を、加入者識別 (IMSI) によって検出し、該加入者識別 (IMSI) が、加入者局 (UPTS, DM) によって加入者識別モジュール (SIM) から読みとられかつインターフェース (DSS1+) を介し送信されることを特徴とする、請求項 1 に記載の方法。

【請求項 3】 別の通信網 (CN) に到達した保護パラメータ (SPAR) を、付加的に加入者データベース (DB) に記録することを特徴とする、請求項 1 又は 2 に記載の方法。

【請求項 4】 加入者データベース (DB) が別の通信網 (CN) に登録された加入者のホーム・データベースであることを特徴とする、請求項 3 に記載の方法。

【請求項 5】 インターフェース (DSS1+) を介し保護パラメータ (SPAR) のそれぞれ 1 つ又は複数のセットを要求して伝送し、かつ保護パラメータの別のセットを使用する前に、加入者認証及び／又はコード化を行うことを特徴とする、請求項 1—請求項 4 のいずれか 1 項に記載の方法。

【請求項 6】 移動無線網 (PLMN) が GSM 基準に基づくセル状の移動無線網であり、該移動無線網によって別の通信網 (CN) の加入者のための GSM 保護パラ

メータ (SRES, RAND, KC) を準備することを特徴とする、請求項 1—請求項 5 のいずれか 1 項に記載の方法。

【請求項 7】 別の通信網 (CN) の加入者のための無線加入者局 (DM) を使用する場合には、保護アルゴリズムが、無線加入者局と基地局 (BS) との間で空気を介し送信されるべき情報をコード化するための手段を有していることを特徴とする、請求項 1—請求項 6 のいずれか 1 項に記載の方法。

【請求項 8】 加入者を認証するための及び／又は情報をコード化するための装置であって、

移動加入者が、加入者局に含まれた加入者識別モジュール (SIM) によって移動無線網に対し識別され、かつ移動無線網 (PLMN) の少なくとも 1 つの加入者データベースに記録されて認証装置 (AC) に登録され、該認証装置 (AC) から加入者データを保護するため、移動加入者に対しそれぞれ保護パラメータ及び保護アルゴリズムが準備可能である形式のものにおいて、

—移動無線網 (PLMN) がインターフェース (DSS1+) を介して別の通信網 (CN) に接続されており、別の通信網の加入者が、加入者局 (UPTS, DM) の加入者識別モジュール (SIM) によって識別されかつ少なくとも別の通信網 (CN) の加入者データベース (DB) に記録されており、

—別の通信網 (CN) には、別の通信網 (CN) の記録された加入者のための保護パラメータ (SPAR) をインターフェース (DSS1+) を介して要求する手段

(PBX) が設けられており、かつ移動無線網 (PLMN) のそれぞれの認証装置 (AC) には、保護パラメータ (SPAR) を準備する手段が設けられており、更に移動無線網には、移動無線網 (PLMN) の加入者データベースに加入者の記録を行うことなしに、保護パラメータ (SPAR) をインターフェース (DSS1+) を介し別の通信網 (CN) に送信する手段 (MSC) が設けられており、

—別の通信網 (CN) の加入者のための認証及び／又は情報のコード化を、移動無線網 (PLMN) によって受信された保護パラメータに基づいて実行する手段 (PBX) が別の通信網に設けられている

ことを特徴とする装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、請求項 1 及び請求項 8 の上位概念に記載の、加入者を認証するための及び／又は情報をコード化するための方法及び装置に関する。

## 【0002】

【従来の技術】 テレコンレポート (telecom report) 16 巻 (1993)、6 号、326 頁から 329 頁までの論文「汎欧州移動通信における安全第 1」

(Safety First bei europaw  
eiter Mobilkommunikation)  
によれば、国際GSM基準 (Global System for Mobile Communication) に基づくセル・デジタル移動無線網の移動加入者のために、個人的な加入者情報に不正にアクセスしたり悪用したりすることから、加入者データを保護するための方法及び装置が公知である。その際国境を越えて異なる事業者の通信網内で通信することができる移動加入者は、それぞれの通信網に対し、無線加入局内として特徴づけられた加入者識別モジュール (Subscriber Identity Module) によって識別される。移動加入者はSIMカードの受領後認証装置 (Authentication Center) に登録され、該装置から移動加入者のデータを保護するために、それぞれ安全パラメータ及び安全アルゴリズムが準備されている。この目的のために認証装置が1つの安全ユニット (Security Box) を有しており、該安全ユニットに安全アルゴリズムが準備されている。更に伝送のための情報をコード化するための方法 (ciphering) も公知である。

【0003】安全性が極めて重要であるためGSM保護手段、特に保護パラメータ及び保護アルゴリズムは、1つの共通な取り決め (Memorandum of Understanding) に基づき、州を越えて延びている移動無線網基準に接続された通信網事業者と、インフラストラクチャー製造者だけがアクセスできるようになっている。従ってこの保護手段は、移動無線網内だけで使用可能であって、別の通信網、例えば専用網 (Corporate Networks) 内では使用することができない。またGSM基準と別の機能基準、例えば、DECT基準 (Digital Enhanced Cordless Telecommunication) との間では使用不可能であり、又はたとえGSM移動無線網の事業者と別の通信事業者との間に加入者移動性 (Roaming) の保護に関する通信網間の共通な取り決めが存在していても、1つの共通な通信網 (Universal Personal Telecommunication, UPT) 内で使用することは、もちろん不可能である。従ってGSM基準に保護された移動無線網の間だけに取り決めが存在しているか、又は異なった機能基準の通信網での使用は両通信網の加入者データベースの二重加入者登録によってだけ可能である、つまり異なった認証方法によってだけ可能であるようになっている。

#### 【0004】

【発明が解決しようとする課題】本発明の課題は、加入者を認証するための及び／又は情報をコード化するための方法及び装置を提供し、それによって保護手段が、それぞれ移動無線網に接続された別の通信網においても可

能な限りわずかなコストで使用することができるようにすることである。

#### 【0005】

【課題を解決するための手段】本発明では、方法に関しては請求項1に記載の特徴によって、装置に関しては請求項8に記載の特徴によって、それぞれ上記課題を解決することができた。

【0006】保護パラメータには、別の通信網の加入者のために移動無線網から両通信網にわたり接続されたインターフェースが準備されていて、移動無線網におけるこれらの加入者のための加入者登録が、移動無線網の少なくとも1つの加入者データベースで行われなくても良いようになっている。その場合別の通信網の加入者は、それぞれ加入者識別モジュールによって識別されかつ少なくとも別の通信網の加入者データベースに記録される。別の通信網に記録された加入者のための保護パラメータは、インターフェースを介して要求することができ、移動無線網の認証装置によって準備されかつインターフェースを介して別の通信網に伝送される。移動無線網の加入者データベースへの加入者の記録は行われないうままである。これによって、移動無線網の移動加入者呼び出し番号を配信しなくても良いようになり、別の通信網の加入者の管理を行う必要がないという極めて大きな利点が得られる。移動無線網から配信されて別の通信網に受信された保護パラメータに基づいて、別の通信網に登録された加入者のための加入者認証及び／又は情報のコード化が行われる。別の通信網、例えば、ローカル局装置を備えた専用網は、このような形式で、加入者データへの不正なアクセス及び個人的な加入者データの不正な使用及び／又は情報のコード化に対する保護のための対策を自主的に展開することができる。

【0007】しかもこれによって、移動無線網が (保護パラメータの伝送を別にして) 影響を受けないようになっており、かつ別の通信網が、別の通信網における保護パラメータを改定するための極秘保護アルゴリズムを実行する必要がないようになっている。その際有利には、保護パラメータの別のセットを準備するための移動無線網への新しい要求が別の通信網によって開始される前に、先ず保護パラメータの少なくとも1つのセットがインターフェースを介し要求されて伝送され、かつ加入者認証及び情報のコード化が行われるようになっている。

【0008】つまり加入者認証のための、特に基地局と参加者無線局との間で空気を介し伝送される情報のコード化のための、保護パラメータ及び保護アルゴリズムの使用は、別の通信網 (例えば、DECT基準に指示された専用網) を介しての加入者の通信の際にも、また加入者が滞在地を別の通信網の領域から移動無線網の供給領域に変えようとする場合の加入者の通信の際にも、また加入者が滞在地を別の通信網の領域から移動無線網の供給領域に変えようとする場合の加入者の通信の際にも、

これを変換することができるようになっている。

【0009】

【発明の実施の形態】次に本発明を、図に示された実施形態に基づいて詳しく説明する。

【0010】図1には、インターフェースDSS1+を介し移動無線網PLMNに、例えば、GSM基準に基づく移動無線網で接続されている専用網CNで加入者の認証及び情報のコード化を行うためのブロック図が示されている。セル上に構築されたデジタル移動無線網PLMNは、公知のように、無線技術的な部分装置と接続技術的な部分装置とを有している。その際、ホーム加入者データベース（ホーム・レジスタ）で接続技術的な部分装置のビジター加入者データベース（ビジター・レジスタ）の滞在地に依存して登録された移動加入者の無線局が、エアインターフェースを介して、無線技術的な部分装置の多数の基地送信／受信局の内のそれぞれ1つに接続されており、またこれとは逆に接続されている。基地送信／受信局は多数の無線セルに作用を及ぼしており、該無線セルから無線供給のための移動無線網PLMNが、可能な限り多くの加入者を1つにまとめている。

【0011】接続技術的な部分装置は、接続に関連する移動特性的な機能を実現するための無線技術的な部分装置に接続されている。接続技術的な部分装置は、付属のビジター・レジスタVLRを備えた多数の移動接続箇所MSCを有していて、1つの移動接続箇所MSCにそれぞれ役立っている供給領域の加入者データが、実際に滞在する加入者に分散されて一時的に供給されうようになっている。つまり移動加入者のデータは、該データがそれぞれの受け持ち供給領域内に位置する限り、移動無線網PLMNの分散された加入者データとして機能するビジター・レジスタVLRにだけ保存されるようになっている。ビジター・レジスタVLRの外に移動無線網PLMNは、少なくとも一つの図示されていないホーム・レジスタHLRを有している。その際総ての移動加入者の総ての加入者データは、登録の期間の間移動無線網PLMNに集中して供給される。

【0012】認証装置ACはホーム・レジスタHLRに接続されていて、固有のプロセッサと固有の運転装置とを備えた保護ユニット（Security Box）を有している。認証装置ACには、移動加入者が加入者に配分された移動加入者識別IMSIによって登録されており、その際SIMカードの準備に基づく秘密な加入者符号KIも記憶される。SIMカードは加入者識別モジュールSIMであり、該カードSIMによって加入者は移動通信網PLMNに対し識別される。

【0013】加入者識別モジュールSIMを用いて加入者を識別した後、移動加入者の通信網アクセス認可を検査するための加入者認証が行われる。この目的のために認証装置ACには保護パラメータSPARが準備されていて、所定の保護アルゴリズム（例えば、国際GSM基

準に基づいて規定された保護アルゴリズムA3/A8)のための入ロパラメータとして使用されており、該保護アルゴリズムは、他方では、認証のための保護パラメータ（後で説明する、例えば、SRES）ないしは情報をコード化するための保護パラメータ（後で説明する、例えば、KC）を出発パラメータとして供給しうようになっている。しかし州にまたがるGSM移動無線網の事業者は、この保護アルゴリズムに接続されていなくて、独自の保護アルゴリズムを提供することができるようになっている。

【0014】認証装置ACの保護ユニットには、乱数（RAND）と、記憶されたパラメータIMSI及びKIとを使用した保護アルゴリズムA3の結果として、1つの信号（SRES、サインされた応答）が供給される。同じように内方に提供された保護アルゴリズムA3に基づく加入者及び記憶されたパラメータIMSI、KIに基づいて信号（SRES、サインされた応答）を形成する。この両信号が移動無線網PLMNの通信網装置によって、有利には移動接続箇所MSCによって、自己同一性に関し相互に比較される。両信号が一致した場合には加入者認証が効果的に実行される。認証の間保護アルゴリズムA8に基づく加入者識別モジュールSIMでは情報をコード化するための符号（KC）が算出される。移動無線網PLMNの個々の装置が通信することができるように中央プロセッシング装置CCS7（プロセッシング装置番号7）が設けられており、該プロセッシング装置は、移動性に関連した機能処理するための、移動機能特性を備えたユーザ部分MAPを有している。

【0015】専用網CNは少なくとも1つのローカル局装置PBXを有し、該ローカル局装置PBXに加入者は、加入者局UPTSを介して有線接続されているか、又は無線加入者局DM、例えば、GSM基準及びDECT基準に適合した双対モード加入者局と、基地局BSとを介して接続されている。その際加入者局UPTSは、有線接続された加入者の一般的な個人通信及び／又は移動加入者に役立つ通信網（一般的な個人通信、UPT）をバックアップする。両加入者局UPTS、DMは共通であって、専用網CNの加入者が、加入者局に含まれた又は加入者局内に挿入された加入者識別モジュールSIMによって、通信網に対して識別されうようになっている。

【0016】加入者識別モジュールSIMは、加入者のために加入者識別IMSIと、秘密な加入者符号KIとが、例えば、実行される保護アルゴリズムA3に基づいて加入者認証のためにだけ使用される一方で、加入者識別IMSIは、移動無線網PLMNの認証装置ACの確定に役立っており、該認証装置ACによって、認証のための保護パラメータSPAR及び／又は専用網CNの加入者のコード化が準備されるようになっている。専用網は、例えば、多数の位置を備えた企業通信網（Corp

orate Network) から成っており、該位置は相互にネットワーク化されており、かつローカル局装置 PBX に加入者は、導線又は無線通路を介し、例えば、DECT 無線装置の接続によって接続されている。

【0017】ローカル局装置 PBX はそれぞれ 1 つの加入者データベース DB を有し、該データベース DB には、それぞれ登録された加入者のデータが記憶されている。加入者データには、例えば、インターフェース DSS1+ を介して到達可能である移動接続箇所 MSC と、加入者番号 SNR と、認証装置 AC を探索するための、加入者識別モジュール SIM から加入者局 UPTS、DM に受信される加入者識別 IMSI と、加入者によりそれぞれ利用可能である通信サービスを確認するためのサービス手段 SPRO と、認証装置 AC から提供される保護パラメータ SPAR とが含まれており、該保護パラメータ SPAR に基づいて専用網 CN には、認証手順及び／又はコード化手段が自動的に展開されるようになって

いる。

【0018】ローカル局装置 PBX と移動接続箇所 MSC との間に位置するインターフェース DSS1+ を介してインターフェース・プロトコルが使用されており、該プロトコルによって、移動性及び保護性に特有な機能の影響下で保護パラメータ SPAR の交換を行うことができるようになってい

る。インターフェース DSS1+ は、ローカル局装置 PBX から移動接続箇所 MSC に接続するために、例えば、1 つのプロトコルを利用して、保護パラメータ SPAR を伝送するための情報分だけ拡大されている。これによって、例えば、保護アルゴリズムと、準備された専用網 CN の保護パラメータとを導くことができ、かつ無線加入者局 DM 及び基地局 BS の間で空気を介して送信されるべき情報 (例えば、言語及び日付) をコード化するための手段を使用することができるようになってい

る。このためエアインターフェースのための特別な符号 (KC) が必要であり、該符号 (KC) は、保護パラメータ SPAR の部分として移動無線網から要求されかつ認証装置 AC によって準備され又はインターフェース DSS1+ を介して受信されるようになってい

る。

【0019】図 2 には、移動無線網から保護パラメータ SPAR を伝送することによって、専用網 CN に登録された加入者を認証するための経過が示されている。しかもこの場合は加入者記録を、移動無線網 PLMN のホーム・レジスタ HLR で行わなくてもよいようになってい

る加入者局 DM 及び UPTS で加入者の識別を行った後、特に加入者識別 IMSI を含む情報 LUR がローカル局装置 PBX に送信され、該ローカル局装置 PBX によって加入者は、加入者データベース DB に加入者データを記録することにより登録される。滞在地登録が初めて必要である場合、又は別のローカル局装置の領域内には入り込んだ際滞在地登録が必要であるような場合に

は、情報 LUR (位置更新要求) が加入者局から常

に送信される。

【0020】専用網 CN のローカル局装置 PBX から加入者識別 IMSI を備えた情報箇所 SPR が、情報ユニットとして移動接続箇所 MSC のための図 1 のインターフェースを介し、専用網 CN に登録された加入者を認証するための及び／又は保護パラメータを伝送するための要求を信号伝送する。その後移動接続箇所 MSC は、加入者識別 IMSI を備えた情報 SAUI を対応する認証装置 AC のための情報ユニットとして送信する。情報 SAUI (送信認証情報) と一緒に、認証装置で計算されて準備された保護パラメータ SPAR が要求される。その際保護パラメータ SPAR の要求は、通常、識別 IMSI を含む加入者記録が行われることなしに遂行される。また移動加入者呼び出し番号 (MSISDN) の設定も行われない。このため専用網 CN の加入者は、加入者に所属するローカル局装置 PBX においてだけ加入者として登録される一方で、この加入者のホーム・レジスタ HLR には存在していなくて、加入者に対し保護パラメータだけが、認証装置 AC によって通過されたデータとして保管されかつホームローカル局装置として加入者を登録したローカル局装置 PBX の方に送信される。

【0021】このため加入者識別モジュール SIM が、別の通信網、例えば、専用網 CN の通信網事業者に出力され、該モジュール SIM は、対応する加入者データベースに、この例ではローカル局装置 PBX の加入者データベースに、加入者を記録するためにだけ役立っている。通信網事業者又はサービス提供者によって加入者局の利用者に出力された SIM カードが、加入者によって無線加入者局 DM 内又は加入者局 UPTS 内に挿入されて、それぞれの通信網に対し識別されるようになってい

る。この実施形態では、認証装置 AC により専用網 CN への加入者の通信網アクセスのために必要である保護パラメータとして、乱数 RAND と、無線伝送の間に情報をコード化するための符号 KC と、加入者識別モジュール SIM の認可検査のために通信網に対して必要である信号 SRES (サイン応答) とが準備されて、移動接続箇所 MSC へ情報 RSAUI (結果送信認証情報) が発信されるようになってい

る。

【0022】その際、保護パラメータの 1 つ又は複数のセットが準備されており、該保護パラメータは、専用網 CN において先ず認証のために加入者によって処理され、その後で別のセットが保護パラメータによって要求されるようになってい

るので有利である。つまり保護パラメータの多くの異なったセットを移動無線網の認証装置から呼び出すことができ、引き続き専用網において、この例では、付属の加入者データベース DB を備えたローカル局装置 PBX によって前記セットが処理される。移送接続箇所 MSC は、情報 RSAUI の受信後情報 RSP (Result Security Parame

ter) 内に届いたパラメータ RAND, SRES, KC をインターフェースを介し専用網に送信し、ここで前記パラメータは、ローカル局装置 PBX の加入者データベースに保護パラメータ SPAR として記憶される。

【0023】この手順は、認証装置 AC が前もって要求された保護パラメータの 1 つのセットを準備して伝送するその度ごとに繰り返される。ローカル局装置 PBX に登録された専用網 CN の加入者のための加入者認証は、ローカル局装置 PBX によって乱数 RAND を備えた情報 AUR が情報ユニットとしてそれぞれの加入者局 DM 又は UPTS に対し発信されることによって、引き続き自動的に行われる。情報のコード化のために特別な符号 KC が、ローカル局装置 PBX に接続された基地局か、又はコード化された利用情報又は信号化情報を送信するための加入者局か、のどちらかによって利用されている。

【0024】ローカル局装置 PBX は、認証に対する希望を情報 AUR を用いて信号化する。この希望は、信号 SRES を有する情報 RAU の呼び出し装置を備えた加入者局 DM 又は UPTS によって情報ユニットとして応答される。届いた乱数 RAND を基礎にしてそれぞれの加入者局は、SIM カードの準備に基づく秘密加入者コードを用いて信号 SRES が、ローカル局装置 PBX によって加入者データベース DB に記憶された信号 SRE

S と同一であるかどうかを比較する。両信号が一致した場合には、加入者の通信網で保護アルゴリズムを実行する必要なしに専用網 CN に登録された加入者の認証を効果的に行うことができる。移動無線網 PLMN の移動加入者と、別の通信網 CN の加入者とのための別個の認証手順を省くことができる。

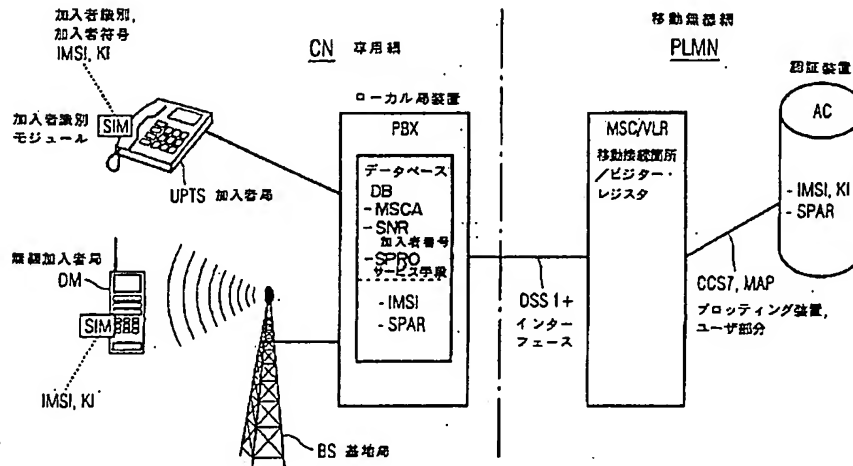
【0025】保護パラメータが、この実施形態では専用網 CN の加入者の認証のための GSM 保護パラメータが、専用網の加入者のための加入者記録を移動無線網の加入者データベースで行うことなしに、前もって要求されて伝送される。この実施形態は、GSM 保護アルゴリズムに基づいて処理される GSM 保護パラメータを準備することに関するが、別の通信網の加入者の認証のための、又は情報のコード化のための、別の保護パラメータ及び保護アルゴリズムも本発明の対象になっている。保護パラメータの伝送のためには、移動無線網と別の各通信網の間にインターフェースプロトコルによるインターフェース接続を行う必要がある。

#### 【図面の簡単な説明】

【図 1】移動無線網に接続された専用網における加入者認証のブロック図である。

【図 2】専用網と移動無線網との間で加入者を認証するための情報の流れ図である。

【図 1】



【図 2】

